

Stephen A. Broome (Bar No. 314605)  
stephenbroome@quinnmanuel.com  
William R. Sears (Bar No. 330888)  
willsears@quinnmanuel.com  
865 South Figueroa Street, 10<sup>th</sup> Floor  
Los Angeles, California 90017  
Telephone: (213) 443-3000  
Facsimile: (213) 443-3100

Lindsay Cooper (Bar No. 287125)  
lindsaycooper@quinnemanuel.com  
50 California Street, Floor 22  
San Francisco, California 94111  
Telephone: (415) 875-6600  
Facsimile: (415) 875-6700

Anil Makhijani (admitted *pro hac vice*)  
anilmakhijani@quinnmanuel.com  
Casey Adams (admitted *pro hac vice*)  
caseyadams@quinnmanuel.com  
51 Madison Avenue, 22<sup>nd</sup> Floor  
New York, New York 10010-1601  
Telephone: (212) 849-7000  
Facsimile: (212) 849-7100

*Attorneys for Defendant TWC  
Product and Technology LLC*

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

JON HART, ALEX DANIELS, and JOSHUA DUNLAP,

Case No. 4:20-cv-03842-JST (AGT)

### **Plaintiffs.**

vs.

TWC PRODUCT AND TECHNOLOGY LLC

## **DEFENDANT TWC'S OPPOSITION TO PLAINTIFFS' MOTION FOR CLASS CERTIFICATION**

The Hon. Jon S. Tigar

Hearing Date: October 6, 2022

Trial Date: None Set

**TABLE OF CONTENTS**

	<u>Page</u>
INTRODUCTION.....	1
I. BACKGROUND.....	3
A. The TWC App Collected Location Data Linked Only to Pseudonymous Device Identifiers, Not Personally Identifying Information .....	3
B. Whether The TWC App Used Precise Location Data To Target Ads Varies Across the Class .....	4
C. The App's Permission Prompts, Privacy Policy, In-App Disclosures, and Other Sources Placed Many Class Members on Notice of TWC's Practices .....	6
D. Dr. Snow's Analysis of Users' Sessions Data Confirms Many Class Members Were Already Aware of TWC's Practices Before It Launched the Blue Screen .....	8
E. Prof. Hanssens' Survey Similarly Confirms That Many Class Members Were Aware of TWC's Practices.....	9
F. The Mischaracterizations in Plaintiffs' Motion for Class Certification.....	10
II. ARGUMENT .....	11
A. Plaintiffs' Lack of Standing Defeats Class Certification on Its Own and Also Creates Typicality and Predominance Issues .....	11
B. Individual Issues of Implied Consent Predominate All Claims .....	13
C. The Unjust Enrichment Claim Cannot be Certified for Additional Reasons.....	16
1. Plaintiffs Fail to Show that TWC Profited Off of All Class Members' Precise Location Data .....	16
2. Plaintiffs' Unjust Enrichment Model Is Untethered to Their Liability Theory and Sweeps In Revenues That Were Not Unjustly Earned .....	18
3. Plaintiffs Cannot Avoid Predominance Issues by Changing Their Theory of Unjust Enrichment to One that Has No Basis in Law .....	20
D. The Constitutional Privacy Claim Cannot be Certified for Additional Reasons.....	20
1. Additional Individual Issues Predominate Plaintiffs' Privacy Claim .....	20
2. Plaintiffs Fail to Offer <i>Any</i> Damages Model For their Privacy Claim.....	22
3. A Nominal or Punitive Damages Class Cannot Be Certified.....	22

1	E.	Individualized Issues Regarding How Users Reacted to TWC's Prompt Defeat Commonality and Predominance.....	23
2	F.	Plaintiffs' Claims Are Not Typical Of Android Users.....	23
3	III.	A CLASS ACTION IS NOT SUPERIOR BECAUSE CLASS MEMBERS CANNOT READILY BE IDENTIFIED .....	24
4	IV.	THE COURT SHOULD DECLINE TO CERTIFY A LIABILITY-ONLY CLASS.....	25
5	V.	CONCLUSION .....	25
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			

**TABLE OF AUTHORITIES**

		<u>Page</u>
	<b>Cases</b>	
4	<i>Am. Acad. of Pediatrics v. Lungren</i> , 16 Cal. 4th 307 (1997).....	21
5	<i>Ang v. Bimbo Bakeries USA, Inc.</i> , 2018 WL 4181896 (N.D. Cal. Aug. 31, 2018).....	23
7	<i>Backhaut v. Apple Inc.</i> , 2015 WL 4776427 (N.D. Cal. Aug. 13, 2015).....	14
9	<i>Bowerman v. Field Asset Servs., Inc.</i> , --- F.4th --- 2022 WL 2433971 (9th Cir. July 5, 2022).....	19, 20, 23
10	<i>Campbell v. Facebook Inc.</i> , 315 F.R.D. 250 (N.D. Cal. 2016) .....	16
11	<i>Castillo v. Bank of Am., NA</i> , 980 F.3d 723 (9th Cir. 2020).....	20
13	<i>Comcast Corp. v. Behrend</i> , 569 U.S. 27 (2013) .....	18, 22
15	<i>Cty. of San Bernardino v. Walsh</i> , 158 Cal. App. 4th 533 (2007).....	22
16	<i>Dytch v. Yoon</i> , 2011 WL 839421 (N.D. Cal. Mar. 7, 2021) .....	13
17	<i>Frank v. Gaos</i> , 139 S. Ct. 1041 (2019) .....	11
19	<i>Franklin v. City of Kingsburg</i> , 2022 WL 815820 (E.D. Cal. Mar. 17, 2022) .....	22
20	<i>Halliburton Co. v. Erica P. John Fund, Inc.</i> , 573 U.S. 258 (2014) .....	11
22	<i>Hill v. Nat'l Collegiate Athletic Ass'n</i> , 7 Cal. 4th 1 (1994).....	13
23	<i>I.C. v. Zynga, Inc.</i> , 2022 WL 2252636 (N.D. Cal. Apr. 29, 2022) .....	11
25	<i>In re Apple iPhone Antitrust Litig.</i> , 2022 WL 1284104 (N.D. Cal. Mar. 29, 2022) .....	18, 19
26	<i>In re Facebook Internet Tracking Litig.</i> , 956 F.3d 589 (9th Cir. 2020).....	20, 21

1	<i>In re Facebook, Inc.</i> , 402 F. Supp. 3d 767 (N.D. Cal. 2019) .....	13, 22
2	<i>In re Google Inc. Gmail Litig.</i> , 2014 WL 1102660 (N.D. Cal. 2014).....	14, 16
4	<i>In re Google Location History Litigation</i> , 428 F. Supp. 3d 185 (N.D. Cal, 2019) .....	21
5	<i>In re Hulu Priv. Litig.</i> , 2014 WL 2758598 (N.D. Cal. June 17, 2014) .....	25
7	<i>In re Toll Roads Litig.</i> , 2018 WL 4952594 (C.D. Cal. July 31, 2018) .....	21
8	<i>IntegrityMessageBoards.com v. Facebook, Inc.</i> , 2021 WL 3771785 (N.D. Cal. Aug. 24, 2021).....	24
10	<i>Moore v. Rodriguez</i> , 2021 WL 2222590 (S.D. Cal. June 2, 2021) .....	22
11	<i>Olean Wholesale Grocery Coop., Inc. v. Bumble Bee Foods LLC</i> , 31 F.4th 651 (9th Cir. 2022).....	11, 12, 17
13	<i>Opperman v. Kong Techs.</i> , 2017 WL 3149295 (N.D. Cal. 2017).....	18, 23
14	<i>Pierce v. Cty. of Orange</i> , 526 F.3d 1190 (9th Cir. 2008).....	24
16	<i>Rahman v. Mott's LLP</i> , 2014 WL 6815779 (N.D. Cal. Dec. 3, 2014) .....	25
17	<i>Stockwell v. City &amp; Cty. of San. Francisco</i> , 2015 WL 2173852 (N.D. Cal. May 8, 2015) .....	25
19	<i>Torres v. Nutrisystem, Inc.</i> , 289 F.R.D. 587 (C.D. Cal. 2013) .....	16
20	<i>TransUnion LLC v. Ramirez</i> , 141 S. Ct. 2190 (2021) .....	13
22	<i>Wal-Mart Stores, Inc. v. Dukes</i> , 564 U.S. 338 (2011) .....	11, 25
23	<i>Ward v. Apple Inc.</i> , 2018 WL 934544 (N.D. Cal. Feb. 16, 2018).....	18
25	<i>Williams v. Apple, Inc.</i> , 338 F.R.D. 629 (N.D. Cal. 2021) .....	18
26	<i>Zinser v. Accufix Research Inst., Inc.</i> , 253 F.3d 1180 (9th Cir. 2001).....	25
28		

1	<b>Rules and Statutes</b>
2	Cal. Civ. Code § 3515 ..... 13
3	Fed. R. Civ. P. 23 ..... 11
4	Fed. R. Civ. P. 23(b)..... 18, 22, 24
5	<b>Other Authorities</b>
6	2 Newberg on Class Actions § 4:72 (6th ed.) ..... 24
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	

## **INTRODUCTION**

In August 2020, following nearly 20 months of litigation with the People of California (represented by the L.A. City Attorney) *over the exact conduct at issue here*, TWC settled the People’s claims. *See Ex. A (Joint Stip. and Order).*<sup>1</sup> Plaintiffs nevertheless ask the Court to certify a class of California residents based on the same allegations TWC already settled with the People. But the two claims they seek to certify—for unjust enrichment and violation of the right to privacy under the California Constitution—are not certifiable for multiple reasons.

8       First, Plaintiffs lack standing. During the class period, TWC generally did not maintain  
9 personally identifying information of its users; rather, it used device identifiers to preserve  
10 anonymity. Based on the device IDs Plaintiffs produced, there is no evidence that TWC even  
11 collected precise location data from two of the Plaintiffs during the class period. And whether TWC  
12 collected precise location data from the third Plaintiff has not been confirmed. Nor is there evidence  
13 that TWC used any Plaintiff's precise location data for advertising (or any other allegedly improper  
14 purpose). Accordingly, Plaintiffs lack standing and the class cannot be certified. Moreover, the  
15 protracted discovery process required to identify Plaintiffs' historical device IDs used during the  
16 class period—and the resulting one-third success rate of actually locating relevant location data—  
17 confirms that individualized issues of standing pervade the claims of the entire class.

18        *Second*, implied consent defeats all claims, but requires individualized resolution. During  
19 the class period, TWC published a Privacy Policy that expressly disclosed its use and sharing of  
20 location data for advertising (and other commercial purposes). The Privacy Policy was available via  
21 a link on the App’s download pages, from multiple links within the App, and on TWC’s website.  
22 The in-App Privacy Settings page also disclosed the conduct. So did several news articles. Indeed,  
23 TWC’s experts have confirmed that many App users were aware of the conduct and were fine with  
24 it. At trial, TWC would argue that those who used the App while aware of TWC’s practices  
25 impliedly consented and have no claim. But that defense cannot be fairly tried in a class proceeding  
26 because it requires examining individual class members about their knowledge.

<sup>1</sup> “Ex.” cites refer to exhibits to the attached Declaration of Stephen Broome.

1        *Third*, Plaintiffs' unjust enrichment claim implicates myriad additional issues that preclude  
 2 certification. For example, the claim turns on whether TWC unjustly profited from class members'  
 3 precise location data by using it to target the ads they were shown, but the record confirms *most* ads  
 4 shown within the App are targeted based on criteria *other than* precise location. Plaintiffs thus  
 5 cannot show that TWC was unjustly enriched from the class as a whole, and they offer no method  
 6 for identifying class members whose data resulted in TWC's unjust enrichment. Even if they could,  
 7 their unjust enrichment model does not attempt to isolate the extent to which TWC profited from  
 8 precise location data (as opposed to other factors), nor does it include a mechanism for allocating  
 9 the alleged unjust enrichment in proportion to class members' respective harm, which varies widely.

10        *Fourth*, Plaintiffs' constitutional privacy claim similarly requires analysis of factors that are  
 11 not uniform for the class. For example, users who shared their location with the App "Always" are  
 12 differently situated from users who shared their location "Only While Using the App" and used the  
 13 App rarely; users who disabled personalized ads (thereby preventing the use of their location data  
 14 for ad targeting) are differently situated from users who did not; and users whose precise location  
 15 data was analyzed for purposes of placing them in advertising segments are differently situated from  
 16 users whose data was not. Plaintiffs do not grapple with these issues. Nor do they proffer a damages  
 17 model for this claim; instead, they argue—without support—that unjust enrichment is a remedy for  
 18 *both* claims. The weight of authority holds that *no* damages are available for a constitutional privacy  
 19 claim, and this Court should not create new precedent endorsing Plaintiffs' novel theory.

20        *Fifth*, because Plaintiffs used only the iOS version of the App, their claims are not typical  
 21 of users of the Android version. Plaintiffs claim they were deceived because the iOS version's  
 22 location prompt made a misrepresentation. Mot. 2. But the Android prompt—which TWC did not  
 23 create and could not modify—made no representations; it merely asked for permission. TWC's  
 24 defenses vis-à-vis Android App users cannot be fairly tried because there are no Android users  
 25 among the named Plaintiffs. Thus, at a minimum, no class including Android users can be certified.

26        *Finally*, a class action is not superior to other means of litigating the case—it would create  
 27 an administrative nightmare. As Plaintiffs' own experience demonstrates, merely *confirming* that an  
 28 individual is a member of the class requires taking a forensic image of their device to locate

1 historical device IDs. This procedure clearly cannot be implemented for the class as a whole.

2 **I. BACKGROUND**

3 **A. The TWC App Collected Location Data Linked Only to Pseudonymous Device**  
**Identifiers, Not Personally Identifying Information**

4  
5 The App is available for download on Android and iOS devices and provides users with  
6 state-of-the-art weather forecasts, alerts, and other real-time weather data. Ex. B (Rouse Decl.) ¶¶ 5-  
7 7. The Android and iOS operating systems (“OS”) can determine the precise geographic latitude  
8 and longitude of a mobile device through location services such as GPS sensors. *Id.* ¶ 9. The OS  
9 collects this data regardless of whether a user has the App installed. *Id.* ¶¶ 9-10; Ex. C (Trotz Dep.)  
10 81:22-84:5. The OS displays a “permission prompt” to which the user must consent before the OS  
11 will allow an app to access precise location data. Ex. B (Rouse Decl.) ¶ 11. If a user consents, the  
12 App accesses the data and provides automatically-localized weather data and alerts. *Id.* ¶ 12.

13 The App does not allow users to create profiles that include names or other identifying  
14 information.<sup>2</sup> *Id.* ¶ 58; Ex. D (Smith Decl.) ¶¶ 10-12. Each installation of the App is associated with  
15 a pseudonymous Advertising ID (“AdID”) randomly assigned to a device by the device’s OS (*i.e.*,  
16 by Android or iOS). Ex. B (Rouse Decl.) ¶ 59. [REDACTED]

17 [REDACTED]  
18 [REDACTED] Ex. C (Trotz  
19 Dep.) at 34:8-40:14. Thus, [REDACTED]

20 [REDACTED] *Id.* at 35:21-38:9. That is especially true since,  
21 as Plaintiffs acknowledged to the Court, “AdIDs can and do change” over time. Dkt. 126 at 4.

22 [REDACTED]  
23 [REDACTED]  
24 Ex. D (Smith Decl.) ¶¶ 5-11. TWC was thus [REDACTED]

---

25  
26 <sup>2</sup> Until May 2018, TWC App users had the option to create a profile and enter certain contact  
27 information. *Id.* ¶ 58. Very few users actually created profiles. In March 2018, only 4.5% of the  
28 monthly active users (“MAU”) on TWC’s iOS App and 3.9% of the MAU on TWC’s Android App  
had profiles. *Id.*; *see also* Ex. D (Smith Decl.) ¶ 12. Plaintiffs do not allege that they created a profile.

1 [REDACTED] Ex. C (Trotz Dep.) at 34:8-38:8.

2 **B. Whether The TWC App Used Precise Location Data To Target Ads Varies**  
 3 **Across the Class**

4 The App costs TWC [REDACTED] per year to operate but is available for free.  
 5 Dkt. 143-11, Pl. Ex. 12 (Clayton Dep.) 190:5-18. As Dr. Jonah Berger (Associate Professor of  
 6 Marketing, the Wharton School) explains, the App, like many other apps, is funded by showing  
 7 users ads that can be targeted based on a variety of criteria. Ex. E (Berger Rep.) ¶¶ 18-19, 22-24;  
 8 Ex. F (Jones Decl.) ¶ 5. Unless a user has paid to access a premium version without ads, ads appear  
 9 in the App alongside its content. [REDACTED]

10 [REDACTED]

11 [REDACTED] Ex. C (Trotz Dep.) 149:18-151:8 Ex. E (Berger Rep.) ¶¶ 25-26.

12 Plaintiffs challenge TWC's use of their "precise" location data. Mot. 1; Dkt. 73 (First  
 13 Amended Complaint) ¶ 35; Ex. G (Pl. Responses to Rog 6). "Precise" location data means the  
 14 latitude and longitude coordinates collected from a device, and differs from coarse location data,  
 15 such as a [REDACTED]

16 [REDACTED] Ex. C (Trotz Dep.) at 64:23-65:3-17. Plaintiffs do not claim a  
 17 privacy interest in coarse location data.

18 Plaintiffs presume that *all* of the ads TWC displays are targeted based on precise location  
 19 data, but in reality most ads use [REDACTED], and very few  
 20 use precise location data. Ex. C (Trotz Dep.) 120:15-121:9; Ex. H (Zeng Decl.) ¶¶ 10-11. Instead,  
 21 many ads are targeted based on [REDACTED]

22 [REDACTED]

23 [REDACTED]. Ex. H (Zeng Decl.) ¶ 10; Ex. C (Trotz Dep.)  
 24 80:13-81:21; Ex. E (Berger Rep.) ¶¶ 45-49. Still other "contextual" ads are targeted based on the  
 25 [REDACTED]

26 [REDACTED] Ex. I (Bartlett Rep.) ¶ 62; Ex. H (Zeng Decl.) ¶ 10. In fact, "a user's precise  
 27 location ... is rarely a valuable targeting variable." Ex. E (Berger Rep.) ¶ 45; Ex. C (Trotz Dep.)  
 28 120:15-121:9. Advertisers typically seek to reach a *broad* audience, while targeting an ad using

1 precise location necessarily limits the audience. Ex. E (Berger Rep.) ¶¶ 46-49. This is true for both  
 2 programmatic and direct sales ads.

3 ***Programmatic Ads.*** [REDACTED]

4 [REDACTED]. Ex. J (Trotz Decl.) ¶¶ 43-60; Ex. H (Zeng  
 5 Decl.) ¶¶ 10-12. [REDACTED]

6 [REDACTED], and the evidence in the  
 7 record indicates that they did not—even if it was available. Ex. E (Berger Rep.) ¶¶ 52-54.  
 8 [REDACTED]

9 [REDACTED] .” Ex. J (Trotz Decl.) ¶¶ 53, 60. [REDACTED]  
 10 [REDACTED]. *Id.* ¶ 64.

11 ***Direct Sales Ads.*** When TWC used location data for advertising, in [REDACTED]

12 [REDACTED] Ex. C (Trotz Dep.) 114:1-17; Ex. E (Berger  
 13 Rep.) ¶ 57. Conversely, “[REDACTED]” were “[REDACTED]  
 14 [REDACTED].” Ex. C (Trotz Dep.) 120:15-121:9.<sup>3</sup> Even when TWC used precise location data to  
 15 target ads, [REDACTED]

16 [REDACTED] ” *Id.* at 81:22-84:5, 87:17-88:11; Ex. E (Berger Rep.) ¶ 58. Indeed, [REDACTED]

17 [REDACTED]  
 18 [REDACTED]. Pl. Ex. 8 at 67:3-69:3; Ex. J (Trotz Decl.) ¶ 15. [REDACTED]

19 [REDACTED] Ex. F (Jones Decl.) ¶ 5.

20 JFX had numerous privacy safeguards. Contrary to Plaintiffs’ assertions (Mot. 1), TWC did  
 21 not pass identifying information about individual users to advertisers through JFX. [REDACTED]

22 [REDACTED]  
 23 [REDACTED]  
 24 [REDACTED]

25 \_\_\_\_\_  
 26 <sup>3</sup> Plaintiffs cite deposition testimony from TWC witness Joey Trotz that precise location data is  
 27 “[REDACTED]” to suggest it is often used for advertising, but Mr. Trotz merely explained  
 that [REDACTED]

28 [REDACTED] ” Dkt. 143-8 (Pl. Ex. 8) at 146:5-148:3.

1 [REDACTED]  
 2 [REDACTED].” *Id.* ¶ 11. “As a  
 3 further layer of protection, TWC salted and hashed the identifiers associated with user location data  
 4 before sending the data to [REDACTED]. As a result of this process, [REDACTED]

5 [REDACTED]” *Id.* ¶ 12.  
 6 [REDACTED]  
 7 [REDACTED]. See Ex. J (Trotz Decl.) ¶¶ 8, 10; Ex. D (Smith Decl.)  
 8 ¶¶ 13-14. [REDACTED]

9 [REDACTED]  
 10 [REDACTED]. *Id.* Plaintiffs provide no  
 11 evidence that any of *their* data was monetized through JFX, or that they were placed in a JFX  
 12 audience.

13 Moreover, users had the option to disable location-targeted ads at any time. Ex. B (Rouse  
 14 Decl.) ¶¶ 27, 40-46. They could do so at the operating system level by disabling personalized ads.  
 15 *Id.* They could also disable location-targeted ads within the App itself. *Id.* ¶¶ 27, 46.

16 In short, whether TWC used the precise location data of a given class member for advertising  
 17 varies from user to user—but for the large majority of them, TWC did not. Plaintiffs offer no  
 18 methodology for identifying putative class members whose precise location data was monetized.

19 **C. The App’s Permission Prompts, Privacy Policy, In-App Disclosures, and Other**  
**Sources Placed Many Class Members on Notice of TWC’s Practices**

21 During the class period, the first time a user opened the App, they saw a prompt that  
 22 requested permission to access their device’s location. *Id.* ¶¶ 17, 32-37. The prompt was generated  
 23 by the device’s OS and required consent to allow the App to access location data. *Id.* ¶¶ 17-18, 32-  
 24 37. The Android prompt came pre-supplied by the OS and could not be modified. *Id.* ¶ 37. Apple  
 25 supplied the initial text of the iOS prompt but required developers to add text. *Id.* ¶ 16.

26 If the user declined consent, the App could not access location data. *Id.* ¶¶ 10-11. If iOS  
 27 users clicked “Only While Using the App,” the OS gave TWC access only when the App was open,  
 28 and if the App requested location data while the App was open only in the background, a new prompt

would display re-requesting access. *Id.* ¶¶ 21-23; Ex. K (Egelman Dep.) 186:18-187:23. If an iOS or Android user selected “Always Allow” or “Allow,” respectively, the App regularly accessed location and provided automatically-localized weather data and alerts. Ex. B (Rouse Decl.) ¶¶ 20-21, 38-39. Plaintiffs allege they only ever used the iOS App and selected “Only While Using the App.” Ex. L (Pl. Responses to Rog. No. 3).

Throughout the class period, TWC’s Privacy Policy explained how TWC used location data. The Privacy Policy in effect from January 2017 through December 2018, for example, stated:

We also collect location information ... so that we can offer you certain location-based services (such as severe weather alerts through our mobile applications), *provide advertisements that are relevant to your geographic location*, and conduct analytics to improve the services . . . . In the event you allow location information collection through your mobile device, we may collect *precise geographic location information*. . . . Depending on your mobile device’s operating system, we typically receive the latitude and longitude of your mobile device, as well as date and time . . . . When your personal data is collected on the Services, it may be shared with selected third parties who assist us with our business operations, with the provision of the Services, *with our marketing or advertising campaigns*, or in delivering you the features and functionality that you have requested.

Ex. M (TWC00001069, at ’71-74) (emphasis added). The Privacy Policy further explained that location information collected may be used to “understand user behavior, [and] *target and measure the effectiveness of advertisements.*” *Id.* at ’73. Another version of the Privacy Policy effective December 2018 disclosed that “we may also provide to Ad Partners . . . information [that] may include data about . . . physical places users have visited.” Ex. N (TWC0000094, at ‘106). The Privacy Policy also disclosed that TWC may “retain your information for as long as your account is active or as needed to provide the Services.” *Id.* at ‘107; Ex. B (Rouse Decl.), at Ex. T.

The Privacy Policy was available for users to review through: (1) a link posted on the App’s download pages, (2) various links within the App, including within the Settings menu, and (3) on TWC’s website (weather.com). *Id.* ¶ 47. Thus, Plaintiffs’ claim that “[t]here was no direction to TWC’s Privacy Policy during [the App’s] onboarding process” (Mot. 2) is false—there was a link to the Privacy Policy on the download page. *Id.*; Rouse Exs. A-I. The Privacy Policy was viewed hundreds of thousands of times during the class period. Ex. D (Smith Decl.) ¶¶ 13-17.

In addition, in May 2018, TWC introduced a “Privacy Settings” screen stating: “Allowing

1 access to your device’s location provides you with the most accurate weather forecasts, severe alerts,  
 2 *geographically relevant ads*, and content. *We may also share location data with partners*, as  
 3 described in our privacy policy.” Ex. B (Rouse Decl.) ¶¶ 64-66. The Privacy Settings screen included  
 4 a “Learn More” button that displayed a page providing similar information. *Id.* ¶ 66.

5 On January 24, 2019, TWC revised the iOS App’s location-access permission prompt to  
 6 specifically mention the use and sharing of location data for advertising. Ex. B (Rouse Decl.) ¶ 67.  
 7 TWC was unable to modify the Android App’s location-access permission prompt because, as  
 8 mentioned above, Android supplied the text and did not permit modification. *Id.*

9 On April 24, 2019, TWC released a new version of the App for both iOS and Android that  
 10 added a “Blue Screen” to the onboarding process. *Id.* ¶¶ 68-72. The Blue Screen: (1) specifically  
 11 disclosed the App’s use and sharing of location data for advertising; (2) provided a link to the App’s  
 12 Privacy Policy; (3) provided a “Learn More” link to a page that further describes the App’s use and  
 13 sharing of location data for advertising; and (4) required users to click “I Understand” before they  
 14 could proceed to use the App. *Id.* ¶ 72. TWC showed the Blue Screen to all users who downloaded  
 15 the App on or after April 24, 2019, *and to all pre-existing users* when they updated to the latest  
 16 version of the App (which typically happens automatically).<sup>4</sup> *Id.* ¶¶ 68-73.

17 **D. Dr. Snow’s Analysis of Users’ Sessions Data Confirms Many Class Members**  
**Were Already Aware of TWC’s Practices Before It Launched the Blue Screen**

19 TWC’s vendor, Localytics, maintained records of the location permission settings of the  
 20 App’s daily active users (“Sessions Data”). This data provided daily information regarding whether  
 21 active users were sharing access to their device’s location-based services. Ex. P (Cyr Decl.) ¶¶ 4-  
 22 14. Through the Sessions Data, it is possible to determine the percentage of active users who  
 23 consented or declined to share location data on a day-to-day basis.

24 The Sessions Data can be used to test whether events such as TWC’s introduction of new

---

25  
 26 <sup>4</sup> Approximately 75% of existing iOS App users updated the App within 17 days after the release  
 27 of the April 24, 2019 version (version 10.9) of the iOS App and thus were presented with the Blue  
 28 Screen and the second revised permission prompt. Approximately 75% of existing Android users  
 updated the App within 28 days after the release of the April 24, 2019 version (version 9.5.0) and  
 thus were presented with the Blue Screen. Broome Decl. Ex. O (Snow Rep.) ¶¶ 48, 58 & n.42.

1 prompts in January and April 2019—which disclosed the information allegedly omitted from the  
 2 prior versions of the prompts that Plaintiffs challenge—had an effect on the rate at which users opted  
 3 to share their location with the App. If Plaintiffs were correct that the prior prompts deceived class  
 4 members, one would expect the rate of location sharing to sharply decrease upon the launch of the  
 5 new prompts. By contrast, if class members were generally aware of TWC’s practices (*e.g.*, because  
 6 they read the Privacy Policy), one would expect the rate to remain stable.

7 TWC retained Dr. Snow, a leading expert in the field of statistics, to analyze these issues.  
 8 Ex. O (Snow Rep.) ¶¶ 22-23. His analysis shows, *inter alia*, that following TWC’s January and  
 9 April 2019 revisions to the prompts to specifically mention the use and sharing of location data for  
 10 advertising (and, in the case of the Blue Screen shown to all new *and existing* users, requiring users  
 11 to click “I Understand”), there was no material change in the rate at which users shared their location  
 12 data with the App. Snow Rep. § V.A. Data on other metrics, such as App usage levels, downloads  
 13 of the App, and uninstalls of the App also show no material change. *Id.* §§ V.B-D.

14       **E. Prof. Hanssens’ Survey Similarly Confirms That Many Class Members Were**  
 15       **Aware of TWC’s Practices**

16       Dr. Dominique Hanssens, Professor of Marketing at UCLA’s Anderson School of  
 17 Management, conducted surveys of actual App users, and separately of non-App users, to determine  
 18 whether users were aware of how the TWC App and apps like it used their data, how they viewed  
 19 such uses, and what users expected TWC to do with their data based on the App’s prompts during  
 20 the class period. The surveys show that users: (1) expected the free version of the App to use their  
 21 location to show them targeted ads; (2) would go to the App’s privacy policy or privacy settings to  
 22 learn more about its use of their data; and (3) consider it beneficial to share their location in order  
 23 to receive targeted weather forecasts. Ex. Q (Hanssens Rep.) ¶¶ 16-20, 43-44, 51, 53.

24       Plaintiffs’ expert, Serge Egelman, agrees: his research shows users *prefer* targeted ads, do  
 25 not consider them intrusive, and would prefer to receive location targeted ads than pay a fee of \$0.99  
 26 to use an app without them. Ex. R (Serge Egelman et al., *Choice Architecture & Smartphone*  
 27 *Privacy: There’s a Price for That* (2013)), at 19. Dr. Egelman’s research also found that “location  
 28 sharing is not viewed as dangerous in comparison to the other risks of using applications,” ranks in

1 the “bottom half of risks” for smartphone users, and that “the privacy community should refocus  
 2 their efforts on *other types of smartphone data that evoke higher levels of user concern*, such as text  
 3 messages, photos, and contacts.” Ex. S (Serge Egelman et al., *I’ve Got 99 Problems, But Vibration*  
 4 *Ain’t One: A Survey of Smartphone Users’ Concerns* at 6 (2012)).

5 **F. The Mischaracterizations in Plaintiffs’ Motion for Class Certification**

6 Plaintiffs’ motion relies heavily on mischaracterizations of the record and unsupported  
 7 assertions. Plaintiffs assert (Mot. 2) that “at least 85% of Android users were allowing location  
 8 services … and more than 45% of iOS users had selected ‘Always’ for location permissions,” which  
 9 is allegedly “far higher than most applications.” But the exhibits they cite—Exs. 3 and 12—do not  
 10 support these contentions. They also assert (Mot. 3) that “TWC also provided location data to IBM’s  
 11 Watson Advertising arm before the two operations were merged” in 2016, but the exhibits they cite  
 12 show the opposite. Mot. 3 (Pl. Exs. 9 & 14). In fact, [REDACTED]

13 [REDACTED] Ex. H (Zeng Decl.) ¶ 12.

14 Plaintiffs cite to their complaint for the assertion that “[t]here was no direction to TWC’s  
 15 Privacy Policy during [the TWC App] onboarding process or signal that users should seek more  
 16 information” (Mot. 2), but the record establishes that the TWC App download pages on both the  
 17 Google Play and Apple App stores prominently displayed a link to the Privacy Policy throughout  
 18 the class period. *See* Ex. B (Rouse Decl.) ¶¶ 16, 47.

19 Even worse, Plaintiffs omit an entire section of the Privacy Policy they submit (Dkt. 141-  
 20 36, Pl. Ex. 34), excluding a section called “How We Share or Disclose Your Information”—which  
 21 states “*We may share … location data, advertising identifiers … with advertisers and other third*  
 22 *parties,*” Ex. T (TWC0000035), at ‘039 (emphasis added)—and then misleadingly argue that the  
 23 Privacy Policy fails to disclose that TWC may share location data with third parties. Mot. 9-10.

24 Plaintiffs wrongly assert that TWC “sought to build ‘Portraits’ or ‘customer profiles’” of  
 25 individual users when Plaintiffs know well that is not accurate. Mot. 4. The cited document makes  
 26 clear that these “portraits” were simply [REDACTED]

27 [REDACTED]  
 28 [REDACTED]. Pl. Ex. 16. They were not “portraits” of individual users.

1 Plaintiffs likewise conflate what TWC purportedly “sought” to do with how TWC *actually*  
 2 used precise location data, often based on citations to early-stage marketing materials that describe  
 3 aspirational business plans TWC never implemented. Mot. 3. As explained by Joey Trotz, TWC’s  
 4 former Global Head of Advertising Technology, TWC’s actual use of precise location data proved  
 5 short-lived and far more limited than Plaintiffs suggest. Ex. J (Trotz Decl.) ¶¶ 8-15. Indeed, while  
 6 Plaintiffs suggest that TWC “sought to sell” data to “financial services companies,” the cited  
 7 deposition testimony states only that this [REDACTED].

8 Pl. Ex. 9 (Glackin Dep.) 60:2-14. Plaintiffs also do not show any class members’ data was used.

9 In short, close scrutiny of Plaintiffs’ purported “evidence” is warranted.

10 **II. ARGUMENT**

11 A plaintiff must “actually *prove*—not simply plead—that his putative class satisfies each  
 12 requirement of Rule 23.” *Halliburton Co. v. Erica P. John Fund, Inc.*, 573 U.S. 258, 275 (2014).  
 13 Plaintiffs bear the burden of showing, by a “preponderance” of “admissible evidence,” that they  
 14 have met Rule 23’s requirements. *Olean Wholesale Grocery Coop., Inc. v. Bumble Bee Foods LLC*,  
 15 31 F.4th 651, 664-65 (9th Cir. 2022). The Court must conduct a “rigorous analysis” to ensure  
 16 Plaintiffs meet that burden, rather than simply accepting Plaintiffs’ allegations as true. *Wal-Mart*  
 17 *Stores, Inc. v. Dukes*, 564 U.S. 338, 350-51 (2011).

18 **A. Plaintiffs’ Lack of Standing Defeats Class Certification on Its Own and Also**  
 19 **Creates Typicality and Predominance Issues**

20 “In a class action, at least one named plaintiff must have standing.” *I.C. v. Zynga, Inc.*, 2022  
 21 WL 2252636, at \*6 (N.D. Cal. Apr. 29, 2022) (citing *Frank v. Gaos*, 139 S. Ct. 1041, 1046 (2019)).  
 22 None of the Plaintiffs has standing for the claims asserted here.

23 *First*, there is no objective evidence that TWC even *collected* precise location data from  
 24 Plaintiffs Hart and Dunlap during the class period (let alone used the data for advertising). TWC  
 25 searched its systems for the relevant IDs provided by Plaintiffs and found *no* location data for Hart’s  
 26 IDs and location data for Dunlap’s IDs only for the period March 17, 2019 through October 30,  
 27 2020—*i.e.*, *after the class period* (and after Dunlap would have seen the Blue Screen). Dkt. 87-1  
 28 (Partin Decl.) ¶¶ 5-11. Hart and Dunlap try in vain to establish standing by pointing to their own

1 assertions that they “downloaded the TWC App and allowed permission to their location.” Mot. 6.  
 2 But even if these self-serving assertions are credited, downloading the App and giving location  
 3 permission does not necessarily result in TWC *collecting* their data during the class period,  
 4 particularly where, as here, the users allegedly selected the Only While Using setting. *Id.* ¶ 16; Ex.  
 5 L (Pl. Responses to Rog No. 3). If Hart and Dunlap used the App infrequently or not at all during  
 6 the class period, for example, the App may not have collected any data. Or perhaps Plaintiffs shared  
 7 their location only on older devices for which they no longer retain the IDs. Or perhaps they are not  
 8 telling the truth. It is extremely difficult to tell, not least because Hart’s tablet device is a decade old  
 9 and appears to be running a version of the TWC App that TWC stopped supporting years ago, and  
 10 Dunlap’s device was manufactured in September 2019, *after* TWC’s allegedly unlawful conduct  
 11 ended, highlighting the inherent difficulties in determining class member standing here. Broome  
 12 Decl. ¶ 34; Dkt. 87-1 (Partin Decl.) ¶ 11.

13 Plaintiffs’ reliance on purported “forensic images of their phones [that] reflects that the  
 14 operation by which TWC collects location data was run on each of them,” is misplaced. Mot. 6  
 15 (citing Pl. Exs. 24-26). The documents Plaintiffs cite are not “forensic images” but rather  
 16 demonstratives allegedly produced by a “vendor” that Plaintiffs refused to even identify let alone  
 17 produce for deposition. Broome Decl. ¶¶ 35-44. Plaintiffs refused to produce forensic images to  
 18 TWC for examination (despite repeated requests); the purported “evidence” has not been  
 19 authenticated; and no expert has explained what “geod/com.weather.TWC” even means. *Id.* This  
 20 falls short of Plaintiffs’ obligation to show they have standing by a “preponderance” of “admissible  
 21 evidence.” *Olean*, 31 F.4th at 664-65.

22 *Second*, although TWC eventually identified location data associated with IDs provided by  
 23 Plaintiff Daniels, the initial IDs Daniels provided generated no location data, Dkt. 87-1 (Partin  
 24 Decl.) ¶¶ 5-11, and Plaintiffs have not proven that the second set of IDs provided (only after TWC  
 25 moved to dismiss for lack of standing, Dkt. 87) exist on his device. To date, Plaintiffs have refused  
 26 to participate in a process that would allow TWC to confirm that fact. Broome Decl. ¶¶ 35-44. Thus,  
 27 the record is devoid of evidence that TWC collected precise location data from a single Plaintiff.

28 *Third*, given that Plaintiffs indisputably consented to the collection through the permission

1 prompts, they must show that TWC *used* the data for advertising to establish standing. Plaintiffs fail  
 2 to provide *any* evidence that TWC did so. TWC served ads through more than two dozen  
 3 programmatic ad exchanges that did not *access* precise location data, and Plaintiffs have presented  
 4 no evidence that [REDACTED]  
 5 [REDACTED] . Ex. J (Trotz Decl.) ¶¶ 43-60 Ex. H (Zeng Decl.) ¶¶ 10-12. The  
 6 record indicates they did not. Ex. E (Berger Rep.) ¶¶ 52-54. And for direct sale ads, [REDACTED]  
 7 [REDACTED] . Ex. C (Trotz Dep.) 120:15-121:9. It is thus entirely possible that, even if  
 8 TWC collected precise location data from Plaintiffs, they were shown ads targeted based only on  
 9 criteria other than precise location. Plaintiffs fail to show otherwise.

10 Even if Plaintiffs attempt to address these defects by adding new evidence on reply, which  
 11 is improper, *see Dytch v. Yoon*, 2011 WL 839421, at \*3 (N.D. Cal. Mar. 7, 2021), standing issues  
 12 would still preclude certification because the need for Plaintiffs to proffer additional evidence—  
 13 obtained by forensic analysis of their devices—to sustain *their own* claims confirms standing cannot  
 14 be resolved without individualized proceedings to determine whether (1) TWC in fact collected  
 15 location data associated with device IDs belonging to a class member, and (2) used that class  
 16 member’s data to target ads. *See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2208 (2021) (“Every  
 17 class member must have Article III standing in order to recover individual damages.”).

18       **B.     Individual Issues of Implied Consent Predominate All Claims**

19       Certification should also be denied because issues of implied consent predominate. Under  
 20 California law, one “who consents to an act is not wronged by it.” Cal. Civ. Code § 3515. Consent  
 21 is an element of Plaintiffs’ constitutional privacy claim. *Hill v. Nat’l Collegiate Athletic Ass’n*, 7  
 22 Cal. 4th 1, 26 (1994) (“the plaintiff in an invasion of privacy case … must not have manifested by  
 23 his or her conduct a voluntary consent”). Consent is also a defense to Plaintiffs’ unjust enrichment  
 24 claim. *In re Facebook, Inc.*, 402 F. Supp. 3d 767, 803 (N.D. Cal. 2019) (dismissing unjust  
 25 enrichment claim “as to the plaintiffs who consented” to the conduct).

26       “Individual issues regarding [implied] consent are likely to overwhelmingly predominate  
 27 over common issues” where “there is a panoply of sources from which [] users could have learned  
 28 of” the challenged conduct, including “[the defendant’s] disclosures, third-party disclosures, and

1 news articles.” *In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at \*16-17 (N.D. Cal. 2014); *see*  
 2 *also Backhaut v. Apple Inc.*, 2015 WL 4776427, at \*14 (N.D. Cal. Aug. 13, 2015) (individualized  
 3 issues of implied consent predominated where “numerous sources of information, including  
 4 disclosures by Defendant, [] could have put some proposed class members … on notice of the  
 5 alleged interceptions.”). Here, class members might have learned of the challenged conduct because  
 6 they: (1) read TWC’s Privacy Policy; (2) read the in-App Privacy Settings page, (3) read public  
 7 news articles that notified them that their data could be used for advertising, *see* Exs. U-Z, or (4)  
 8 were otherwise aware of how TWC used their data based on familiarity with the App or similar  
 9 apps, *see* Ex. O (Snow Rep.), §§ V.A-D; Ex. Q (Hanssens Rep.) ¶¶ 47-49. TWC is entitled to defend  
 10 itself at trial by arguing that the particular combination of disclosures and information a given class  
 11 member reviewed placed her on notice of the challenged conduct. It would then be up to the jury to  
 12 determine whether that user impliedly consented. That “intensely factual question” cannot be  
 13 accomplished in a class proceeding. *See Gmail*, 2014 WL 1102660, at \*17.

14 Plaintiffs’ argument (at 9) that the “Privacy Policy did not explicitly disclose” how TWC  
 15 used precise location data ignores its plain language. Although Plaintiffs assert (without citation)  
 16 that the Privacy Policy did not disclose “how TWC would store historic location information, how  
 17 it would use this information to deliver advertisements based on historic location,” and various other  
 18 alleged uses, the Privacy Policy in fact disclosed *all* of the conduct about which Plaintiffs complain.  
 19 *See supra* § I.C; Ex. B (Rouse Decl.) ¶¶ 47-52, Exs. P-T.

20 Indeed, all three Plaintiffs admitted that any user who read the Privacy Policy “would have  
 21 understood that one reason TWC collects location information is to provide advertisements that are  
 22 relevant to the user’s geographic location.” Ex. AA (Dunlap) 188:11-190:21; *see also* Ex. BB  
 23 (Daniels) 114:16-115:21; Ex. CC (Hart) 122:15-123:17. TWC should thus be able to cross examine  
 24 each of the many class members who read the Privacy Policy on whether *they* understood it (like  
 25 Plaintiffs did), which cannot be done in a class action.

26 Plaintiffs’ argument that the Privacy Policy is irrelevant because it “was—at most—a  
 27 browsewrap agreement” (at 9) conflates the defenses of express and implied consent, which are  
 28 “analytically distinct.” *Gmail*, 2014 WL 1102660, at \*19. It also wrongly assumes that TWC is

1 relying on constructive notice, rather than *actual* notice, and that not a single class member actually  
 2 read the Privacy Policy. Mot. 9. In fact, Dr. Hanssens' survey showed that "most users" would check  
 3 the TWC Privacy Policy or the App's privacy settings if they wanted to understand TWC's uses of  
 4 location data. Ex. Q (Hanssens Rep.) ¶¶ 18, 51. And data produced by TWC confirms that hundreds  
 5 of thousands of users did so. Ex. D (Smith Decl.) ¶¶ 13-17.

6 Plaintiffs also ignore that even class members who did not read the Privacy Policy would  
 7 have learned that TWC may use location data for advertising if they viewed the in-App Privacy  
 8 Settings page, Ex. B (Rouse Decl.) ¶¶ 24-25, 27, 46, 62-64, or read one of the many public articles  
 9 that discussed that TWC may use location data for advertising.<sup>5</sup> For example, a 2016 Wall Street  
 10 Journal article reported: "Specific data from the Weather Co. that pairs the exact location and  
 11 climate a woman is in allows for highly targeted advertising."<sup>6</sup> Indeed, Plaintiff Dunlap testified that  
 12 he learned apps may have been tracking his location through "a YouTube search" and "a  
 13 documentary." Ex. AA (Dunlap Dep.), at 60:6-61:10. Other users doubtless did too.

14 Still other class members were aware that apps like the TWC App might use their precise  
 15 location data for advertising because they had a general understanding that apps operate this way.  
 16 Dr. Hanssens' surveys confirm this. The vast majority of respondents shown the prompts in effect  
 17 during the class period believed it was "likely" or "extremely likely" that the App would display  
 18 targeted ads based on current or historical location. Ex. Q (Hanssens Rep.) ¶¶ 16-17, 43-44. A study  
 19 co-authored by Plaintiffs' expert, Dr. Egelman, corroborates this: it found that "[m]any participants  
 20 explicitly associated the presence of ads with a degree of tracking and data collection they would

---

21  
 22  
 23     <sup>5</sup> Ex. U (Michelle Manafy, *The Weather Company's JOURNEYfx location-based ads see the bigger*  
     *picture*, Digital Content Next (Oct. 18, 2016)); Ex. V (David Kaplan, *The Weather Company Rolls*  
     *Out Location Marketing Platform to Anticipate Consumers' Movements*, Geo Marketing (Oct. 13,  
     2016)); *see also* Ex. W (Kelly Liyakasa, *Beyond Paid Media: Weather Co. Rolls Out Journey FX*  
     *Data Offering with a Boost from IBM*, AdExchanger (Oct. 13, 2016); Ex. X (Street Fight Mag,  
     *Weather Company Continues Data Expansion with First-Party Location-Targeting Platform* (Oct.  
     13, 2016); Ex. Y (Richard Harris, *Your Apps Know Where You Were Last Night, and They're Not*  
     *Keeping it Secret*, N.Y. Times (Dec. 10, 2018)).

24  
 25  
 26  
 27     <sup>6</sup> Ex. Z (Katherine Rosman, *Weather Channel Now Also Forecasts What You'll Buy*, Wall Street  
     Journal (Aug. 14, 2016)).

1 expect from an app.”<sup>7</sup> *See Campbell v. Facebook Inc.*, 315 F.R.D. 250, 266 (N.D. Cal. 2016)  
 2 (“individual issues of implied consent [] predominate … due to the media reports on the practice”).

3 Dr. Snow’s analyses further show that implied consent cannot be resolved on a class-wide  
 4 basis. They show that even when TWC added even more explicit new disclosures about the use and  
 5 sharing of location data for advertising, the rates at which users shared their location with the App,  
 6 and used, downloaded and uninstalled the App, did not materially change. Ex. O (Snow Rep.),  
 7 §§ V.A-D. That users did not change their behavior upon reviewing the allegedly omitted  
 8 information and being required to click “I Understand” to continue using the App demonstrates that  
 9 many users were already aware of TWC’s use of their precise location data. *Id.* ¶ 27; § V.A.

10 In short: “A fact-finder, in determining whether Class members impliedly consented, would  
 11 have to evaluate to which of the various sources each individual user had been exposed and whether  
 12 each individual ‘knew about and consented to the interception’ based on the sources to which she  
 13 was exposed.... This fact-intensive inquiry will require individual inquiries into the knowledge of  
 14 individual users.” *Gmail*, 2014 WL 1102660, at \*18; *See also Torres v. Nutrisystem, Inc.*, 289 F.R.D.  
 15 587, 594-95 (C.D. Cal. 2013) (denying certification because “[t]he issue of whether class members  
 16 consented ... would also require a detailed factual inquiry for each class member”).

17       C.     **The Unjust Enrichment Claim Cannot be Certified for Additional Reasons**

18           1.     **Plaintiffs Fail to Show that TWC Profited Off of All Class Members’**  
 19                   **Precise Location Data**

20 Plaintiffs contend that “the Premium targeting used to monetize location data in TWC’s  
 21 Premium advertising business are [sic] known as Geo-Hyperlocal and JourneyFX,” and that “TWC  
 22 specifically charged more for advertisements with” these targeting layers. Mot. 19. Plaintiffs fail to  
 23 show, however, that all class members were exposed to the Geo-Hyperlocal or JourneyFX targeting  
 24 layers. The exhibit they cite (Pl. Ex. 7) shows these were just two of over a dozen potential targeting  
 25  
 26

---

27           7   Ex. DD (Catherine Han, Serge Egelman, et al., *The Price is (Not) Right: Comparing Privacy in*  
 28                   *Free and Paid Apps*, Proceedings on Privacy Enhancing Technologies (2020) (3):222–242), at 235.

1 layers.<sup>8</sup> See also Ex. EE (Nam Decl.) ¶ 10.

2 Plaintiffs further contend that the Google and Twitter/MoPub programmatic exchanges  
 3 utilized precise location data. Mot. 20. But Plaintiffs do not cite any evidence for this contention  
 4 and the evidence in the record indicates otherwise. *Supra* at 5. Even if Plaintiffs could establish that  
 5 the Google and Twitter programmatic exchanges utilized precise location data, Plaintiffs cannot  
 6 show that all class members were shown ads through those exchanges—as opposed to the many  
 7 other exchanges TWC used during the class period that never accessed precise location. See Ex. H  
 8 (Zeng Decl.) ¶¶ 7-11. Nor can Plaintiffs show that the ads shown to users through the Google and  
 9 Twitter programmatic exchanges were targeted based on precise location for *any* user, let alone all  
 10 class members. Class members whose precise location data was not used for targeting lack standing.  
 11 See *Olean*, 31 F.4th at 669 n.14 (“When a class is defined so broadly as to include a great number  
 12 of members who for some reason could not have been harmed by the defendant’s allegedly unlawful  
 13 conduct, the class is defined too broadly to permit certification.”) (citation omitted).

14 As demonstrated in the Berger Report, the report of Hristina Bartlett (Vice President,  
 15 Analysis Group), and the Rouse Declaration, TWC made *no profits at all* from many class members’  
 16 precise location data, including because (1) TWC only showed them ads that were targeted using  
 17 criteria other than precise location data; (2) they used the App so infrequently that they were never  
 18 shown *any* ads based on their location (whether precise or coarse); or (3) they disabled personalized  
 19 ads. Ex. I (Bartlett Rep.) §§ III.A-B; Ex. E (Berger Rep.) § VIII; Ex. B (Rouse Decl.) ¶¶ 24-26, 46;  
 20 Ex. K (Egelman Dep.) 112:9-16 (describing as “realistic” that “somebody might download the app  
 21 and go through the prompt and then never use the app again”). None of these class members were  
 22 “injured” for purposes of an unjust enrichment claim. And Plaintiffs’ expert Ms. Thompson admitted  
 23 she had “***done no analysis***” of how to avoid compensating these uninjured class members. Ex. FF  
 24 (Thompson Dep.) 58:9-15 (emphasis added). Thus, “Plaintiffs cannot meet their predominance  
 25 burden because they rely on an unsound methodology, which cannot reliably demonstrate which

---

27  
 28<sup>8</sup> Pl. Ex. 7 also explains that “[REDACTED]” “[REDACTED]  
 [REDACTED],” not based on their precise location. Pl. Ex. 7 (emphasis added).

1 members, and how many, were injured.” *In re Apple iPhone Antitrust Litig.*, 2022 WL 1284104, at  
 2 \*16 (N.D. Cal. Mar. 29, 2022); *Williams v. Apple, Inc.*, 338 F.R.D. 629, 642 (N.D. Cal. 2021)  
 3 (“[N]ot only is it likely that the putative class contains many members who never suffered the  
 4 alleged contractual breach, but also it is infeasible to determine who those injured class members  
 5 are.”); *see also Opperman*, 2016 WL 3844326, at \*13 (denying certification where class contained  
 6 members “who have suffered no injury at all”).

7 Plaintiffs cannot kick the issue of proving class-wide injury down the road by claiming it  
 8 relates only to the merits. Mot. 5. Rule 23 assigns Plaintiffs the burden of showing they can establish  
 9 class-wide unjust enrichment *now*. *See Comcast Corp. v. Behrend*, 569 U.S. 27, 33 (2013); *see also*  
 10 *Ward v. Apple Inc.*, 2018 WL 934544, at \*3 (N.D. Cal. Feb. 16, 2018) (denying certification where  
 11 plaintiffs did not offer a “data-driven model” establishing injury and damages on a class-wide basis).

12 **2. Plaintiffs’ Unjust Enrichment Model Is Untethered to Their Liability**  
**Theory and Sweeps In Revenues That Were Not Unjustly Earned**

14 “[A] model purporting to serve as evidence of damages in [a] class action must measure only  
 15 those damages attributable to that theory [of liability]. If the model does not even attempt to do that,  
 16 it cannot possibly establish that damages are susceptible of measurement across the entire class for  
 17 purposes of Rule 23(b)(3).” *Comcast*, 569 U.S. at 35. Here, Plaintiffs offer Ms. Thompson’s model,  
 18 which, among other defects described in the concurrently-filed Thompson *Daubert*, would sweep  
 19 in revenues that have nothing to do with the challenged conduct and thus were not unjustly earned.

20 Ms. Thompson’s model fails to identify the *portion* of revenues associated with the  
 21 challenged conduct (*i.e.*, the monetization of precise location data). Rather, the model takes all  
 22 revenues from all ads TWC displayed through four identified channels that *may* use precise location,  
 23 regardless of whether (1) the ads were displayed on the TWC App (as opposed to the TWC website),  
 24 or (2) precise location was actually used to target the ads that contributed to the revenues. This  
 25 would result in wildly inflated class-wide unjust enrichment and compensate class members for  
 26 benefits TWC realized independent of the challenged conduct. Ex. F (Jones Decl. ¶ 5); Ex. I (Bartlett  
 27 Rep.) § III.C; *see also Opperman v. Kong Techs.*, 2017 WL 3149295, at \*12 (N.D. Cal. 2017) (Tigar,  
 28 J.) (denying certification where Plaintiffs’ damages expert’s methodology “would overstate

1 Plaintiffs' damages" by "encompass[ing] a variety of concepts that are not at issue in the case").

2 This problem arises because, contrary to Plaintiffs' contentions (Mot. 19-20), [REDACTED]

3 [REDACTED]  
4 [REDACTED] Ex. F (Jones Decl.) ¶¶ 5-16; Ex. I (Bartlett Rep.) ¶¶ 52-54. Indeed, even  
5 when an ad is targeted based *in part* on precise location data, [REDACTED]  
6 [REDACTED]. Ex. H (Zeng Decl.) ¶ 10; Ex. J (Trotz Decl.) ¶ 14. Plaintiffs thus offer no workable method  
7 for determining the portion of the revenue associated with the monetization of precise location data,  
8 because no method exists. *Bowerman v. Field Asset Servs., Inc.*, --- F.4th --- 2022 WL 2433971, at  
9 \*9 (9th Cir. July 5, 2022) (reversing certification where plaintiffs failed to show that class members  
10 "necessarily suffered damages traceable to" defendant's alleged misconduct).

11           **3. Plaintiffs Fail to Propose A Method for Allocating Unjust Enrichment**

12           As further explained in the Thompson *Daubert* (at § III.D), Plaintiffs' model fails to identify  
13 any method for allocating the alleged unjust profits to class members in proportion to their harm (if  
14 any). *See In re Apple iPhone Antitrust Litig.*, 2022 WL 1284104, at \*16 ("At the class certification  
15 stage, plaintiffs may rely on aggregate damages estimates, but must also establish that 'there is a  
16 method, common across the class, for arriving at individual damages' to survive the predominance  
17 inquiry.") (citation omitted). The extent to which TWC profited from individual class members'  
18 precise location data varies significantly. For some class members (*e.g.*, those who use the app rarely  
19 and were only shown, or primarily shown, ads targeted using other criteria) it may be zero or a  
20 nominal amount; for others, who used the app frequently and thus were shown more ads, the amount  
21 may be more significant. Plaintiffs fail to propose any method for determining (1) whether ads  
22 shown to a given user were targeted using precise location data; (2) how much TWC profited from  
23 targeting ads based on precise location data (if any was used) for that user; or (3) whether the user  
24 was a member of the class (*i.e.*, a California resident) at the time such ads were shown. Plaintiffs'  
25 expert admits she has not considered how to allocate the alleged unjust profits in light of these  
26 problems. Ex. FF (Thompson Dep.), at 24:22-25:5; *see* Ex. I (Bartlett Rep.) ¶¶ 89-100.  
27  
28

1           **3. Plaintiffs Cannot Avoid Predominance Issues by Changing Their Theory**  
 2           **of Unjust Enrichment to One that Has No Basis in Law**

3           In a futile effort to avoid predominance issues, Plaintiffs now contend that, for their unjust  
 4           enrichment claim, “[t]he injury to the class members was *not* the amount of revenue TWC was able  
 5           to generate from each individual user”; instead: “The harm was brought about from their being  
 6           subject to TWC’s uniform practices without disclosure.” Mot. 17 (emphasis added). Plaintiffs cite  
 7           no case supporting such a novel theory of unjust enrichment. It is even less clear how Plaintiffs  
 8           intend to calculate damages from “exposure to [] general geolocation policies.” *Id.* They offer no  
 9           model for doing so. Their damages expert, Ms. Thompson, purports to provide a method for  
 10          calculating only traditional unjust enrichment—the amount TWC profited from using class  
 11          members’ data in four specified advertising channels. Pl. Ex. 36 (Thompson Rep.), at 3-4.

12          Moreover, Plaintiffs later argue that “TWC specifically charged more for advertisements  
 13          with the [precise location] targeting layers at issue,” and that such revenue “is directly tied to the  
 14          theory of liability.” Mot. 19. But TWC could only be unjustly enriched by targeting layers using a  
 15          class member’s precise location data *by showing that class member an ad targeted with the relevant*  
 16          *“layer.”* Ex. H (Zeng Decl.) ¶ 10; Ex. J (Trotz Decl.) ¶ 14; Ex. I (Bartlett Rep.) ¶ 46. Thus, despite  
 17          Plaintiffs’ protestations (at 17), “differences in the number of advertisements shown to an individual  
 18          class member or the targeting applied to any such advertisements *does* [] defeat predominance.” See  
 19          *Bowerman*, 2022 WL 2433971, at \*8 (9th Cir. July 5, 2022) (certification improper despite  
 20          plaintiff’s assertion that all class members were subject to “uniform” practice because “liability to  
 21          any class member … would implicate highly individualized inquiries”); *Castillo v. Bank of Am.,*  
 22          *NA*, 980 F.3d 723, 732 (9th Cir. 2020) (affirming denial of certification where “a large portion of  
 23          the proposed class was never exposed to the challenged” conduct).

24           **D. The Constitutional Privacy Claim Cannot be Certified for Additional Reasons**

25           **1. Additional Individual Issues Predominate Plaintiffs’ Privacy Claim**

26          To prevail on this claim, Plaintiffs must show: “(1) there exists a reasonable expectation of  
 27          privacy, and (2) the intrusion was highly offensive.” *In re Facebook Internet Tracking Litig.*, 956  
 28          F.3d 589, 601 (9th Cir. 2020). Individualized issues predominate for both elements.

1       ***Reasonable Expectation of Privacy:*** “[T]his element contemplates an inquiry into whether  
 2 there is something in the *particular circumstances* in which an alleged intrusion of privacy arises  
 3 that demonstrates the plaintiff has no reasonable expectation of privacy *in that context.*” *Am. Acad.*  
 4 *of Pediatrics v. Lungren*, 16 Cal. 4th 307, 338 (1997) (emphasis added). Here, those “particular  
 5 circumstances” turn on numerous individualized issues specific to how each class member used the  
 6 App. These include the facts that: (1) iOS and Android users saw different location-sharing prompts  
 7 (Plaintiffs’ claims are based on the iOS version), (2) some users saw the Privacy Policy, in-App  
 8 Settings page, or were otherwise aware that apps may use location data for ad targeting; and (3)  
 9 TWC collected very different amounts of data from iOS users depending on the setting they selected  
 10 (“Always” vs. “Only While Using”) and how frequently they used the App.

11       Indeed, Plaintiffs argue that “[a] reasonable expectation is more likely to be found where  
 12 ‘the amount of data allegedly collected was significant.’” Mot. 13 (citing *Facebook Internet*  
 13 *Tracking*, 956 F.3d at 603). But here, the amount of data collected for a given user would be minimal  
 14 if, for example, she used the Only While Using setting, opened the App infrequently, and closed the  
 15 App when done. *See In re Google Location History Litigation*, 428 F. Supp. 3d 185, 198 (N.D. Cal.,  
 16 2019) (dismissing constitutional privacy claim because collection of location data was “not  
 17 automatic” and did not result in “*all* of Plaintiffs movements [] being collected,” but only “specific  
 18 movements or locations” depending on “how often [Plaintiffs] use Google’s services”; “[s]uch ‘bits  
 19 and pieces’ do not meet the [requisite] standard of privacy”). By contrast, the amount of data may  
 20 be significant if the user selected “Always,” but the very name of that setting placed the user on  
 21 notice of the frequency at which data would be collected.

22       Plaintiffs further contend that “when analyzed to render ‘Portraits’ of users and home  
 23 locations, the sensitivity of the data is heightened” (Mot. 14), but they fail to show this was done  
 24 classwide. It was not. Ex. D (Smith Decl.) ¶ 14. Ex. And Plaintiffs’ conclusory assertion that a  
 25 reasonable person would not expect TWC to monetize precise location data is belied by Prof.  
 26 Hanssens’ Survey, Dr. Snow’s findings, and the findings of their own expert. *See supra* §§ I.D, E.  
 27 Thus, “[t]he reasonable expectation of privacy of class members here would turn on a slew of  
 28 potential factors.” *See In re Toll Roads Litig.*, 2018 WL 4952594, at \*7 (C.D. Cal. July 31, 2018).

1       ***Highly Offensive:*** Individualized issues would overwhelm this element too, including  
 2 whether users selected “Always” or “Only While Using,” whether they disabled personalized ads  
 3 (thereby preventing the use of location data for advertising), or whether they reset their AdIDs.  
 4 Plaintiffs’ own expert, Dr. Egelman, conducted a survey showing that “improper location sharing is  
 5 not viewed as dangerous in comparison to the other risks of using applications,” confirming there is  
 6 an *absence* of class-wide evidence that users find TWC’s conduct “highly offensive.” Ex. S at 6.

7                   **2. Plaintiffs Fail to Offer Any Damages Model For their Privacy Claim**

8       Plaintiffs’ “model does not even attempt” to “measure only those damages attributable to”  
 9 their constitutional privacy claim. *See Comcast*, 569 U.S. at 35. Rather, Ms. Thompson purports to  
 10 have developed a “Classwide Unjust Retained Benefit Model.” Pl. Ex. 36 at 3. She testified that she  
 11 was *not* asked to develop a model for calculating damages for the constitutional privacy claim. Ex.  
 12 FF (Thompson Dep.) 32:2-33:14. Accordingly, Plaintiffs’ model “cannot possibly establish that  
 13 damages [for their privacy claim] are susceptible of measurement across the entire class for purposes  
 14 of Rule 23(b)(3).” *Comcast*, 569 U.S. at 35.

15      Plaintiffs contend that Ms. Thompson’s model (which they call a “disgorgement model”) “is  
 16 tied to their theory of liability on *both* of their claims.” Mot. 18 (emphasis added). But it is clearly  
 17 an unjust enrichment model and Plaintiffs cite no case holding that disgorgement of unjust profits  
 18 is a remedy for a constitutional privacy claim.<sup>9</sup> *See* Mot. 18-20 (citing only *In re Facebook Inc.*, 402  
 19 F. Supp. 3d at 803 (unjust enrichment claim), and *Cty. of San Bernardino v. Walsh*, 158 Cal. App.  
 20 4th 533, 543 (2007) (breach of fiduciary duty” claim against corrupt officials)).

21                   **3. A Nominal or Punitive Damages Class Cannot Be Certified**

22      Plaintiffs cannot skirt their failure to prove class-wide injury or damages by seeking  
 23 “nominal” or “punitive” damages. Even those damages would run headlong into the problem that

---

25      <sup>9</sup> Indeed, Plaintiffs acknowledge that “the availability of damages” for this claim is uncertain. Mot.  
 26 10. This Court previously declined to rule on that issue. Dkt. 45 at 9. Since then, “the weight of the  
 27 case law” has continued to hold “that only injunctive relief is available.” *Franklin v. City of  
 28 Kingsburg*, 2022 WL 815820, at \*9 (E.D. Cal. Mar. 17, 2022); *Moore v. Rodriguez*, 2021 WL  
 2222590, at \*20 (S.D. Cal. June 2, 2021) (same). TWC intends to raise this issue at summary  
 judgment, if necessary, consistent with the Court’s prior guidance. Dkt. 45 at 9.

1 Plaintiffs cannot identify class members who were injured, such that they would in theory be entitled  
 2 to damages of any kind. *See Opperman*, 2016 WL 3844326, at \*13 (denying certification of nominal  
 3 damages class that “contains members who have suffered no injury at all”); *Bowerman*, 2022 WL  
 4 2433971, at \*8 (rejecting plaintiffs’ attempt to “mischaracterize an issue of individualized *liability*  
 5 as an issue of individualized *damages*”); *see also Ang v. Bimbo Bakeries USA, Inc.*, 2018 WL  
 6 4181896, at \*16 (N.D. Cal. Aug. 31, 2018) (“courts in this district have not been inclined” to allow  
 7 parties to avoid flaws in their damages model by resorting to a request for nominal damages).

8       **E. Individualized Issues Regarding How Users Reacted to TWC’s Prompt Defeat**  
 9       **Commonality and Predominance**

10 Plaintiffs’ contend that the case presents common issues because the App’s location  
 11 permissions prompts were “functionally uniform” throughout the class period. Mot. 2. But their own  
 12 expert, Dr. Egelman, disagrees. He testified that “***we can’t assume that***” the prompts in effect  
 13 during the class period were “uniform” and that consumers may have had *different* reactions to the  
 14 prompts. Ex. K (Egelman Dep.) 71:10-73:16. Indeed, his primary criticism of Drs. Snow and  
 15 Hanssens (albeit a baseless one) is that *they* assume the prompts in effect during the class period  
 16 were uniform. *Id.* at 66:8-68:10. Dr. Egelman further testified that the use of the word “personalized”  
 17 in one of the prompts may have indicated an advertising purpose to some users, and absent a rigorous  
 18 empirical study, “we can’t know for sure” how consumers reacted to the prompts, let alone whether  
 19 consumers viewed them as “identical.” *Id.* 26:19-27:20. But as Mr. Egelman noted, the type of  
 20 “scientifically rigorous study” necessary to confirm Plaintiffs’ hypothesis that the prompts were  
 21 uniform throughout the class period “wasn’t done, ***so it is hard to draw any conclusions.***” *Id.* 26:19-  
 22 27:20. By offering what their own expert described as “just speculation,” Plaintiffs fall short of  
 23 satisfying their burden under Rule 23. *Id.* 27:21-28:7.

24       **F. Plaintiffs’ Claims Are Not Typical Of Android Users**

25 Plaintiffs used only the iOS version of the App. Ex. L (Pl. Responses to Rog No. 3). They  
 26 claim that, in the iOS permission prompt, “TWC uniformly represented that by sharing their location  
 27 users would receive ‘personalized’ or ‘accurate’ weather and alerts, and did not disclose the true  
 28 purpose of its acquisition of location data.” Mot. 8. The Android prompt, however, did not make

1 this or any other representation. Rather, as Plaintiffs acknowledge (Mot. 2), the Android prompt  
 2 simply asked a question: “Allow the Weather Channel to access this device’s location?” Android  
 3 users thus were not subjected to the alleged misrepresentation. Plaintiffs’ expert testified that one  
 4 should not assume users would have the same expectations upon reviewing either the iOS or  
 5 Android prompts. Ex. K (Egelman Dep.) 26:19-27:20. But TWC cannot effectively make its case  
 6 against Android users because there are none among the putative class representatives. Accordingly,  
 7 to the extent a class is certified, it must exclude Android users. *See IntegrityMessageBoards.com v.*  
 8 *Facebook, Inc.*, 2021 WL 3771785, at \*8 (N.D. Cal. Aug. 24, 2021) (typicality lacking where class  
 9 representatives’ use of interface was not “materially similar to that” of other class members).

10 **III. A CLASS ACTION IS NOT SUPERIOR BECAUSE CLASS MEMBERS CANNOT**  
**READILY BE IDENTIFIED**

11 Rule 23(b)(3) requires that class treatment be a superior way to resolve the dispute. A court’s  
 12 considerations should include “the likely difficulties in managing a class action.” Fed. R. Civ. P.  
 13 23(b)(3)(D). Manageability “is, by far, the most critical concern in determining whether a class  
 14 action is a superior means of adjudication.” 2 NEWBERG ON CLASS ACTIONS § 4:72 (6th ed. 2022)

15 A class action is not superior here due to “expected difficulties identifying class members”  
 16 and their data. *See Pierce v. Cty. of Orange*, 526 F.3d 1190, 1200 (9th Cir. 2008) (affirming  
 17 decertification). TWC does not maintain information that personally identifies class members or  
 18 their residencies. Ex. D (Smith Decl.) ¶ 10. Rather, TWC uses TWC IDs or AdIDs to identify  
 19 devices. *Id.* ¶¶ 5-9. But as Plaintiffs acknowledge, “AdIDs can and do change,” as can TWC IDs.  
 20 Dkt. 126 at 4; Ex. D (Smith Decl.) ¶ 7. AdIDs can easily be reset by the user, and TWC IDs may  
 21 reset whenever a user uninstalls and reinstalls the TWC App for any reason. Ex. D (Smith Decl.)  
 22 ¶ 7. Indeed, when Plaintiffs initially produced their *current* AdIDs and TWC IDs, TWC was unable  
 23 to locate location data from the class period for a single Plaintiff and moved to dismiss for lack of  
 24 standing. Dkt. 87. Only after Plaintiffs’ (unidentified) vendor purportedly conducted forensic  
 25 images of their devices (which Plaintiffs refused to produce), and purportedly located *historical*  
 26 AdIDs, was TWC able to locate location data from the class period for a *single* Plaintiff. This process  
 27 took months. Broome Decl. ¶¶ 35-44. To repeat this process for the entire class is not feasible.  
 28

Nor is self-reporting at claims administration a solution. Self-reporting is unreliable because it is prone to “subjective memory problems,” and “creates incentives for claimants” to fabricate or embellish claims. *See In re Hulu Priv. Litig.*, 2014 WL 2758598, at \*14-23 (N.D. Cal. June 17, 2014) (rejecting self-reporting in case alleging improper transmission of personal data to Facebook). Moreover, TWC is entitled to challenge individual class members’ claims in the same way that it challenges Plaintiffs’ claims. Without a forensic analysis or some other method for confirming TWC actually collected class members’ precise location data and used it for advertising during the class period (which method Plaintiffs do not propose), self-reporting would deprive TWC of the ability to argue that putative class members in fact have no claim. *See Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 367 (2011) (“[A] class cannot be certified on the premise that [defendants] will not be entitled to litigate [their] defenses to individual claims.”).

#### **IV. THE COURT SHOULD DECLINE TO CERTIFY A LIABILITY-ONLY CLASS**

As demonstrated above, many issues going to liability—including standing, consent, damages, and individualized issues pertaining to elements of Plaintiffs’ claims—foreclose certification of even a liability class. *Stockwell v. City & Cty. of San Francisco*, 2015 WL 2173852, at \*9 (N.D. Cal. May 8, 2015) (denying liability class where “the majority of the class would be made up of individuals with no claim for relief”). Indeed, Plaintiffs have not even “devised a plan to resolve this case after the liability phase.” *See Zinser v. Accufix Research Inst., Inc.*, 253 F.3d 1180, 1190 (9th Cir. 2001) (affirming denial of certification because “there was no manageable trial plan adequate to deal with individualized issues”). Certifying a liability class and “allowing myriad individual damages claims to go forward,” after time-consuming liability proceedings that are themselves beset by individualized issues, “hardly seems like a reasonable or efficient alternative, particularly in a case such as this where the average class member is likely to have suffered less than a hundred dollars in damages.” *See Rahman v. Mott’s LLP*, 2014 WL 6815779, at \*9 (N.D. Cal. Dec. 3, 2014), *aff’d* 693 F. App’x 578 (9th Cir. 2017).

#### **V. CONCLUSION**

TWC respectfully requests that the Court deny Plaintiffs’ motion for class certification.

1 DATED: July 28, 2022

QUINN EMANUEL URQUHART & SULLIVAN, LLP

2

3

4

By /s/ Stephen A. Broome

5 Attorney for Defendant TWC Product and Technology LLC

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

## ATTESTATION

I, Lindsay Cooper, am the ECF User whose ID and password are being used to file this document. In compliance with Civil Local Rule 5-1(h)(3), I hereby attest that Stephen Broome has concurred in this filing.

DATED: July 28, 2022

## QUINN EMANUEL URQUHART & SULLIVAN, LLP

By: /s/ Lindsay Cooper

Lindsay Cooper